

the server, and the protected copy of requested data is downloaded from the server to the client in response to the request.

72 2126 38. (New) A method as in claim 30, wherein the program running at the client generates and uploads a request for data from the client to the server, and the protected copy of requested data is downloaded from the server to the client in response to the request.--

REMARKS

Reconsideration and allowance of this application are respectfully requested. Currently, claims 1-8, 12, 14-18, 21 and 28-38 are pending in this application.

Attached hereto is a marked-up version of the changes made to the claims by the current Amendment. The attached is captioned "**Version With Markings to Show Changes Made.**"

Rejections Under 35 U.S.C. §112:

Claims 29 and 31-33 were rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

With respect to claim 29, the Office Action held, "It is an independent claim about a computer program carrier medium, but fails to particularly pointing (sic) out and distinctly claiming (sic) the subject matter that the applicants regards (sic) as their invention (please note that referring to 'claim

28' should not be used for an independent claim).” By this Amendment, claim 29 has been rewritten into independent form. Reference to claim 28 has been deleted.

With respect to claims 31-33 the Office Action held, “They are directed to a method/a server for protecting data; however, the final results after performing these claims are achieving data in their unprotected forms....” Applicant submits that claims 31-33 are in full conformance with 35 U.S.C. §112, second paragraph. In particular, Applicant notes that the “final results” are not merely achieving data in their unprotected forms as alleged by the Office Action, but additionally restricting access to copy and/or save functions of the data in its unprotected form. By restricting or preventing access to copy and/or save functions of the data, the data is “protected.” It is therefore clear that claims 31-33 provide two different types of protection to the data: (1) the data are “protected” during download by encryption, and (2) the data in its unprotected form is “protected” at the client by restricting or preventing access to copy and/or save functions. Accordingly, claims 31-33 clearly recite a method of “protecting data.” Data in its unprotected form is “protected” by restricting or preventing access to copy and/or save functions as required by claims 31 and 32.

Accordingly, Applicant respectfully requests that the rejections of claims 29 and 31-33 under 35 U.S.C. §112, second paragraph, be withdrawn.

Rejections Under 35 U.S.C. §102 and §103:

Claims 1-2, 5-6, 12, 28 and 30-33 were rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Spies et al (U.S. '314, hereinafter "Spies"). Applicant respectfully traverses this rejection.

For a reference to anticipate a claim, each element must be found, either expressly or under principles of inherency, in the reference. Applicant respectfully submits that Spies fails to disclose, or even suggest, each element of the claimed invention. For example, Spies fails to disclose selectively controlling access to copy or save functions at the client in respect of data in its unprotected form, as required by independent claim 1. Independent claims 28 and 30-33 require similar features. For example, Spies fails to disclose restricting or preventing access to copy or save functions of data in its unprotected form.

Spies is directed to a method of cryptographically protecting video content using cryptographic keys to enable secure ordering and transferring of video content from a server (e.g., a video content provider computer) to a client (e.g., a user's set top box). Spies is particularly concerned with ensuring that if video content is intercepted in transit between a server and a client, or when in possession of user (e.g., when stored on a DVD or upon arrival at a user's set-top box or other computer unit), pirate copies cannot be made. This is achieved by Spies through a particular method of storing and exchanging cryptographic keys so that when the video content is accessible, it is encrypted in a way that would be almost impossible to decrypt without access to the appropriate keys.

In particular, Spies discloses an integrated circuit (IC) card arranged to interface with a user's set-top box to store the essential decryption capabilities (see, e.g., col. 8, lines 26-43) with respect to particular video content ordered by the user. Those capabilities are downloaded to the IC card once the order has been validated. The IC card may also be arranged to implement at least a part of a decryption program stored in the IC card to decrypt downloaded encrypted packets so that the ordered video content may displayed on the user's display device (e.g., a television).

While Spies discusses preventing unauthorized access to cryptographic keys and ensuring that video content remains in an encrypted form when outside the user's set-top box, Spies fails to disclose any measures to restrict or prevent access to video content within the set-top box. That is, Spies fails to disclose restricting or preventing access to copy or save functions once the data has been decrypted and is in a form that can be sent to a display device for display. Unauthorized access to already decrypted data within the set-top box is not considered at all by Spies to be a problem.

The Office Action alleges that Fig. 12, block 338 and col. 1, lines 45-49 discloses the above claimed features. Applicant respectfully disagrees. Col. 1, lines 45-49 states "On the other hand, when the video is distributed on cassette or DVD, the viewer is considered to have the ability to record and redistribute the video with little difficulty." This portion of Spies has nothing to do with *search* running a program at a client for restricting or preventing access to copy or save functions of data in its unprotected form. Indeed, this portion of Spies

indicates that users can record and redistribute data with little difficulty. If access to copy or save functions is restricted or prevented, a user would likely have a high degree of difficulty copying or saving the data in its unprotected form.

For the above reasons alone, Applicant submits that claims 1-2, 5-6, 12, 28 and 30-33 are not anticipated by Spies.

Claim 1 further requires running a program portion at a client to generate and upload to the server a request for access to data. Claim 1 further requires that this same program portion convert the cryptographically protected data to an unprotected form and selectively control access to copy or save functions of the data in its unprotected form. Claim 1 therefore requires that the same program portion generates and uploads a request for access to data and performs conversion of the cryptographically protected data to an unprotected form.

In contrast, Spies discloses a video purchasing application program or a video on demand (VOD) application program which runs at a user's "viewing computing unit" (see col. 13, line 24 et seq. or col. 15, line 18 et seq.) to enable a user to select a video to be downloaded and to generate an order for the selected video. Spies then discloses performing order validation and key encryption and a downloading process to encrypt and download the ordered video content. However, once the encrypted video content is delivered to the client (e.g., the user's set-top box), Spies discloses using a separate program - a "decryption routine" in the embodiment shown in Fig. 7 or a separate

“decryption unit” in the embodiment illustrated in Fig. 8 - to control perform the decryption of the downloaded data. The decryption routine or decryption unit is therefore not the same program portion or unit as that which (e.g., the portioning application program) generates and uploads the request (order) for access to video data.

Accordingly, Applicant submits that claim 1 is not anticipated by Spies for this additional and independent reason. Similar comments apply to claims 28, 31 and 32 as well as new dependent claims 37 and 38.

Accordingly, Applicant respectfully submits that claims 1-2, 5-6, 12, 28 and 30-33 are not anticipated by Spies and therefore respectfully requests that the rejection of these claims under 35 U.S.C. §102(e) be withdrawn.

Claims 7, 8, 14, 21 and 29 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Spies. Claims 3 and 4 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Spies in view of Rhoads (U.S. ‘978). Claim 15 was rejected under 35 U.S.C. §103 as allegedly being unpatentable over Spies in view of Probst (U.S. ‘899). Claims 17 was rejected under 35 U.S.C. §103 as allegedly being unpatentable over Spies in view of Official Notice. Claim 18 was rejected under 35 U.S.C. §103 as allegedly being unpatentable over Spies in view of Crawford (U.S. ‘651). Claims 3-4, 7-8, 14-18 and 21 depend from claim 1 and claim 29 depends from claim 28. All of the above comments with respect to Spies therefore apply equally to these dependent claims. Neither Rhoads, Probst, Official Notice or Crawford remedies the above deficiencies of Spies with respect to the claimed invention.

Accordingly, Applicant submits that none of these claims are "obvious" under 35 U.S.C. §103 and therefore respectfully requests that the rejection of these claims under 35 U.S.C. §103 be withdrawn.

New Claims:

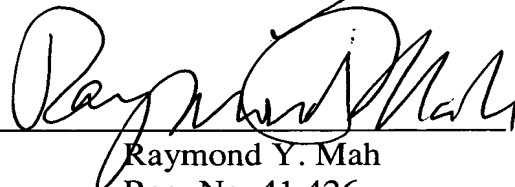
New claims 34-38 have been added to provide additional protection for the invention. Claims 34-36 require restricting or preventing copy or save functions with respect to data in its unprotected form. Applicant therefore respectfully submits that these claims are allowable. Claims 37 and 38 depend from claims 30 and 33, respectively, and therefore are allowable for at least the reasons discussed above.

Conclusion:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Raymond Y. Mah
Reg. No. 41,426

RYM/sl
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703)816-4044
Facsimile: (703)816-4100

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

29. (Amended) A computer program carrier medium containing a computer program which [implements the functions of the server in claim 28 when installed and run on a server.] are executable by a computer to perform method steps for implementing a server, the method steps comprising:

receiving a request for access to a data set;

cryptographically protecting the requested data set; and

generating a program portion for sending to the source of the access request,

wherein said program portion is operable and after the program portion is permitted to run at the source of the access request, in use:

generating a request for access to the cryptographically protected data set;

on receipt of the cryptographically protected data set, converting it into an unprotected form; and

selectively controlling access to copy or save functions in respect of the data set when in said unprotected form.